BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

IPW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Jung-Soo JUNG et al. Docket: 678-1443 (P11789)

Serial No.: 10/822,068 Dated: May 10, 2004

Filed: April 9, 2004

For: **METHOD AND SYSTEM FOR PROVIDING BROADCAST SERVICE USING ENCRYPTION IN A MOBILE COMMUNICATION SYSTEM**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF PRIORITY DOCUMENT

Sir:

Enclosed are certified copies of Korean Appln. Nos. 2003-23002 filed on April 11, 2003 and 2003-23129 filed on April 11, 2003, from which priority is claimed under 35 U.S.C. §119.

Respectfully submitted,

Paul J. Farrell
Registration No. 33,494
Attorney for Applicants

DILWORTH & BARRESE, LLP
333 Earle Ovington Boulevard
Uniondale, New York 11553
(516) 228-8484

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8 (a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postpaid in an envelope, addressed to the: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on May 10, 2004.

Dated: May 10, 2004

Paul J. Farrell

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0023002
Application Number

출 원 년 월 일 : 2003년 04월 11일
Date of Application APR 11, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2004 년 04 월 19 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2003.04.11
【국제특허분류】	H04M
【발명의 명칭】	이동통신 시스템에서 암호화를 이용한 방송 서비스 방법
【발명의 영문명칭】	BROADCASTING SERVICE METHOD USING ENCRYPTION IN MOBILE TELECOMMUNICATION SYSTEM
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이건주
【대리인코드】	9-1998-000339-8
【포괄위임등록번호】	2003-001449-1
【발명자】	
【성명의 국문표기】	송준혁
【성명의 영문표기】	SONG,Jun Hyuk
【주민등록번호】	710321-1046916
【우편번호】	431-070
【주소】	경기도 안양시 동안구 평촌동 19-1블럭 꿈마을 아파트 203동 402호
【국적】	KR
【발명자】	
【성명의 국문표기】	장용
【성명의 영문표기】	CHANG,Yong
【주민등록번호】	700318-1655313
【우편번호】	463-780
【주소】	경기도 성남시 분당구 수내동(푸른마을) 신성아파트 403동 801호
【국적】	KR

【발명자】
【성명의 국문표기】 박도준
【성명의 영문표기】 PARK,Do Jun
【주민등록번호】 701114-1041823
【우편번호】 135-917
【주소】 서울특별시 강남구 역삼2동 진달래아파트 15동 605호
【국적】 KR
【발명자】
【성명의 국문표기】 김대균
【성명의 영문표기】 KIM,Dae Gyun
【주민등록번호】 681003-1690413
【우편번호】 463-773
【주소】 경기도 성남시 분당구 서현동 시범우성아파트 228동 1703호
【국적】 KR
【발명자】
【성명의 국문표기】 배범식
【성명의 영문표기】 BAE,Beom Sik
【주민등록번호】 710821-1009411
【우편번호】 442-809
【주소】 경기도 수원시 팔달구 영통동 955-1 황골마을 주공아파트 121동 1102 호
【국적】 KR
【발명자】
【성명의 국문표기】 임내현
【성명의 영문표기】 LIM,Nae Hyun
【주민등록번호】 730813-1011631
【우편번호】 135-280
【주소】 서울특별시 강남구 대치동 960-15
【국적】 KR
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이건주 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	16	면	16,000 원

【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원
【합계】	45,000	원	

【요약서】

【요약】

본 발명은 이동통신 시스템에서 무선채널을 통해 이동 단말들에게 방송서비스를 제공하기 위한 방법에 대한 것이다. 무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 기지국 또는 패킷 데이터 서비스 노드는 방송 서비스를 제공받으면서 등록 메시지를 전송하는 단말에게 현재 시점에서 유효한 암호화 키를 제공하고, 방송 서버로부터의 방송 데이터를 상기 암호화 키를 가지고 암호화하여 전송한다. 단말은 소정 주기마다 등록 메시지를 생성하여 전송하고 그에 대한 응답으로 기지국 또는 패킷 데이터 서비스 노드로부터 소정 유효시간을 가지는 암호화 키를 포함하는 암호화 정보 메시지를 수신한다. 그리고 방송 서비스 채널을 통해 수신한 방송 데이터를 상기 암호화 키를 가지고 복호화한다. 이러한 본 발명은 무선 구간을 통해 방송 서비스를 제공하는 시스템에서 불법적인 사용자에 의한 방송 서비스의 사용을 방지하고 정확한 과금 정보를 수집할 수 있다.

【대표도】

도 5

【색인어】

Broadcast Multicast Service, PDSN, PCF, AAA, Encryption key, Registration

【명세서】

【발명의 명칭】

이동통신 시스템에서 암호화를 이용한 방송 서비스 방법{BROADCASTING SERVICE METHOD USING ENCRYPTION IN MOBILE TELECOMMUNICATION SYSTEM}

【도면의 간단한 설명】

도 1은 본 발명의 일 실시예에 따른 방송서비스 시스템의 전체 구성을 나타낸 도면.

도 2는 상기 도 1에 나타낸 방송 서비스 시스템의 프로토콜 스택을 나타낸 도면.

도 3은 본 발명의 일 실시예에 따른 단말과 기지국간의 방송형 서비스 절차를 나타낸 메시지 흐름도.

도 4는 본 발명에 따른 위치등록 메시지의 포맷.

도 5는 본 발명의 제1 실시예에 따라 기지국에 의해 등록을 수행하는 동작을 나타낸 메시지 흐름도.

도 6은 본 발명에 따라 암호화 키를 포함하는 데이터 버스트 메시지의 포맷.

도 7은 본 발명의 제2 실시예에 따라 패킷 데이터 서비스 노드(PDSN)에 의해 등록을 수행하는 동작을 나타낸 메시지 흐름도.

도 8은 본 발명에 따라 암호화 키를 포함하는 암호화 정보 메시지의 포맷.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<9> 본 발명은 이동통신 시스템에 관한 것으로서, 특히 무선채널을 통해 이동 단말들에게 방송서비스를 제공하기 위한 방법에 대한 것이다.

<10> 미래의 통신환경은 유선과 무선의 영역구분이나 지역이나 국가의 구분을 초월한 만큼 급변하고 있다. 특히, IMT-2000(International Mobile Telecommunication 2000) 등과 같은 미래 통신환경은 영상과 음성은 물론 사용자가 필요로 하는 다양한 정보를 실시간으로 그리고 종합적으로 제공하는 환경으로 구축되는 추세이다. 이동통신 시스템의 발달은 셀룰러폰(cellular phone)이나 PCS(Personal Communication System) 등의 이동 단말(Mobile Station: MS)에서 단순히 음성통신만을 수행하던 차원에서 벗어나 문자 정보의 전송은 물론, 방송서비스를 시청할 수 있는 정도까지 도달해 있다.

<11> 전형적인 무선통신 시스템에서 방송 데이터의 전송은 단일 전송(Unicast)에 의해 이루어져왔다. 동시에 복수의 단말들에게 동일한 데이터를 전송하여야 하는 방송 서비스의 특성상, 단일 전송은 시스템과 무선 구간에서 자원의 낭비를 가지고 오며 시스템의 부하를 가중시키는 원인이 된다. 따라서 시스템 자원을 절약하면서 고품질의 방송 서비스를 제공하기 위한 다양한 기술이 연구되고 있다.

<12> 현재 3GPP2(3rd Generation Partnership Project 2)에서는 이동통신 시스템에서 방송서비스를 위해 다양한 서비스 매체 및 효율적인 자원이용을 고려하고 있다. 이러한 방송서비스는

이동 단말로부터의 역방향 반환정보 없이 고속의 순방향 데이터를 단방향 송신함으로써 이루어진다. 이는 개념상 일반 텔레비전 방송 서비스와 유사하다고 할 수 있다.

<13> 비-상업적 서비스 차원에서 방송 서비스를 제공한다면 불특정 다수의 단말들이 기지국으로부터 단말 방향으로의 하향 트래픽 채널을 액세스할 수 있도록 하면 된다. 반면에 경제적 이익을 목적으로 하는 상업적 텔레비전 방송 서비스를 사용자들에게 제공하고자 한다면, 시스템은 인증된 단말기들만이 방송을 수신하고 인증되지 않은 단말기들은 방송을 수신할 수 없도록 하여야 하며, 인증된 단말기들이 방송 서비스를 이용한 시간을 측정하여 정확한 요금을 부과하여야 한다. 그런데 종래의 이동통신 시스템에서는 단말이 방송 서비스를 이용하는 시점을 제어할 수 없기 때문에 불법 단말의 방송 서비스 액세스를 제한할 수 없었으며 효율적인 과금이 불가능하였다는 문제점이 있었다.

【발명이 이루고자 하는 기술적 과제】

<14> 따라서 상기한 바와 같이 동작되는 종래 기술의 문제점을 해결하기 위하여 창안된 본 발명은 이동통신 시스템으로 위치등록을 수행하는 이동 단말들에게 방송 서비스를 제공한다.

<15> 본 발명은 이동통신 시스템으로 위치등록을 수행하는 이동 단말들에게 방송 서비스를 위한 암호화 키를 제공한다.

<16> 본 발명은 이동통신 시스템으로 위치등록을 수행하는 이동 단말들에게 방송 서비스를 위해 소정의 유효시간을 가지는 암호화 키를 제공한다.

<17> 본 발명의 일 실시예는, 무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 단말에서 방송 서비스를 제공받는 방법에 있어서,

<18> 상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 생성하여 상기 기지국으로 전송하는 과정과,

<19> 상기 등록 메시지에 응답하여 방송 서비스를 위해 소정 유효시간을 가지는 암호화 키를 포함하는 암호화 정보 메시지를 수신하는 과정과,

<20> 방송 서비스 채널을 통해 상기 기지국으로부터 수신한 방송 데이터를 상기 암호화 정보 메시지에 포함된 암호화 키를 가지고 복호화하는 과정을 포함하는 것을 특징으로 한다.

<21> 본 발명의 다른 실시예는, 무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

<22> 상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 수신하는 과정과,

<23> 상기 등록 메시지에 응답하여 방송 서비스를 위해 소정 유효시간을 가지는 암호화 키를 생성하고 상기 생성된 암호화 키를 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정과,

<24> 상기 패킷 데이터 서비스 노드를 통해 상기 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 한다.

<25> 본 발명의 또 다른 실시예는, 무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국과 상기 패킷 데이터 서비스 노드에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

<26> 상기 기지국에서 상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 수신하고, 현재 시간으로 설정된 단말의 시간 스탬프 정보와 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자를 포함하는 과금 정보를 생성하여 상기 패킷 데이터 서비스 노드로 전송하는 과정과,

<27> 상기 패킷 데이터 서비스 노드에서 상기 기지국으로부터 상기 과금 정보를 수신하여, 방송 서비스를 위해 소정 유효시간을 가지는 암호화 키를 생성하고 상기 생성된 암호화 키를 상기 기지국으로 제공하는 과정과,

<28> 상기 기지국에서 상기 패킷 데이터 서비스 노드로부터 상기 암호화 키를 수신하여, 상기 암호화 키를 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정과,

<29> 상기 패킷 데이터 서비스 노드에서 상기 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 상기 기지국을 통해 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<30> 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것

이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

<31> 후술되는 본 발명은 이동통신 시스템에서 방송 서비스(Broadcast Service: BCS)를 제공함에 있어서, 위치 등록을 수행하는 이동 단말들에게 방송 서비스를 위한 암호화 키(Encryption key)를 제공하는 것이다. 특히 본 발명은 셀룰러 이동통신 시스템에서 이용되는 등록 메시지를 이용하여 시스템과 이동 단말간에 암호화 키를 동기화한다.

<32> 도 1은 본 발명의 일 실시예에 따른 방송서비스 시스템의 전체 구성을 나타낸 것이다.

<33> 상기 도 1을 참조하면, 방송서버(Broadcasting Service Server or Contents Server: CS) 14는 방송서비스를 위한 영상(Video) 및/또는 음향(Sound)을 포함하는 방송 데이터를 패킷 데이터 서비스 노드들(Packet Data Service Node: PDSN) 13을 통해 기지국들(Base Station: BS) 11a,11b로 전달된다. 상기 방송서버 14가 인터넷 등의 패킷 통신 네트워크를 통해 상기 패킷 데이터 서비스 노드 13에 연결되는 경우, 상기 방송 데이터는 압축된 인터넷 프로토콜(Internet Protocol: IP) 패킷의 형태로 생성된다.

<34> 상기 패킷 데이터 서비스 노드 13은 인증 및 과금(Authentification, Authorization and Accounting) 서버 15로부터 패킷 통신의 인증을 위한 사용자 프로파일 정보를 제공받으며 방송 서비스를 위한 과금 정보를 생성하여 상기 인증 및 과금 서버 15로 제공한다. 상기 기지국들 11a,11b는 셀룰러 이동통신 기술분야에서 잘 알려진 기지국 송수신기들(Base Transceiver Subsystems: BTSs) 11a-1, 11a-2, 11b-1,11b-2와 기지국 제어기들(Base Station Controllers:

BSCs) 11a-3, 11b-3을 포함하는 것으로서 패킷 데이터의 통신을 위한 패킷 제어기들(Packet Control Function blocks: PCF) 12a,12b를 통해 상기 패킷 데이터 서비스 노드 13에 연결된다.

<35> 일 예로서, 상기 방송서버 14에 의하여 생성된 방송 데이터를 기지국들 11a,11b로 전달하기 위해서는 IP 멀티캐스트(Multicast)가 이용된다. 상기 기지국들 11a,11b는 상기 방송서버 14로부터 IP 멀티캐스트 데이터를 제공받는 멀티캐스트 그룹(Multicast Group)을 형성한다. 상기 멀티캐스트 그룹의 소속정보(Membership Information)는 상기 기지국들 11a,11b 각각에 연결되는 멀티캐스트 라우터(Multicast Router: MR)(도시하지 않음)에 의하여 유지된다.

<36> 상기 방송 서버 14에서 생성된 IP 멀티캐스트 데이터는 멀티캐스트 그룹을 형성하는 복수의 기지국들 11a,11b에게 브로드캐스팅되고, 상기 기지국들 11a,11b는 상기 IP 멀티캐스트 데이터를 무선 주파수(Radio Frequency: RF) 신호의 형태로 변환하여 해당 서비스영역에서 송출한다.

<37> 도 2는 상기 도 1에 나타낸 방송 서비스 시스템의 프로토콜 스택을 나타낸 것으로서, 여기서 언급하는 계층(Layer)이란 해당 프로토콜에 따른 동작을 수행하는 소프트웨어 블럭 또는 하드웨어를 의미한다.

<38> 상기 도 2를 참조하면, 인터넷 프로토콜(Internet Protocol)을 통해 방송 서비스를 제공받는 단말(MS)은 제1 계층(Layer 1: L1)인 물리계층(Physical Layer)과, MAC(Media Access Control) 계층과, 제2 계층(L2)인 링크(Link) 계층/PPP(Point to Point Protocol) 계층과 제3 계층(L3)인 IP(Internet Protocol) 계층을 기반으로 하고, 사용자 데이터 프로토콜(User Datagram Protocol: UDP)과 실시간 전송 프로토콜(Real-Time Protocol: RTP) 등을 지원하는 운송(Transport) 계층과, MPEG(Moving Picture Experts Group)-4 등을 지원하는 응용(Application) 계층을 더 포함하여 구성된다.

<39> 기지국/패킷 제어기(BS/PCF)는 단말과의 통신을 위한 물리계층과 링크 계층 및 패킷 데이터 서비스 노드(PSDN)와의 통신을 위한 제1 및 제2 계층으로 구성된다. 패킷 데이터 서비스 노드는 기지국/패킷 제어기와의 통신을 위한 제1, 제2 계층 및 PPP 계층과 패킷 데이터 네트워크와의 통신을 위한 제1 및 제2 계층을 기반으로 하고 IP 계층을 더 포함하여 구성된다. 방송 서버는 적어도 하나의 라우터로 이루어진 패킷 데이터 네트워크와의 통신을 위한 제1, 제2 계층 및 IP 계층을 기반으로 하고, 단말에게 제공할 방송 데이터를 생성하고 전송하기 위해 MPEG-4 등을 지원하는 응용 계층과 운송 계층을 더 포함하여 구성된다.

<40> 부가적으로 방송 서버와 단말간에 별도의 암호화를 사용하는 경우 방송 서버와 단말은 방송 데이터의 암호화(encryption) 및 복호화(decryption)를 위한 암호화(Encryption) 계층을 포함하나, 여기에서의 암호화 및 복호화를 위한 암호화 키는 방송 서비스의 초기화시에 방송서비스 파라미터 메시지(Broadcast Service Parameter Message: BSPM) 등을 통하여 제공될 뿐 주기적으로 갱신되는 것이 아니므로 방송 서비스의 인증 및 과금에 적용될 수 없다. 따라서 본 명세서에서는 방송 서버와 단말간의 암호화에 대한 상세한 설명을 생략할 것이다.

<41> 도 3은 본 발명의 일 실시예에 따른 단말과 기지국간의 방송형 서비스 절차를 나타낸 메시지 흐름도이다.

<42> 상기 도 3에서, 전원이 인가되면 단말은 초기화(Initialization)를 수행한 후 방송형 서비스를 수신하기 위해서 자신이 동조되어 있는 주파수 대역(f_{HASH})을 통해 기지국에서 공통 채널로 송신하는 방송서비스 파라미터 메시지(Broadcast Service Parameter Messages: BSPM)를 수신하여 방송형 서비스에 대한 세션 정보를 획득한다. 상기 BSPM은 방송 서비스를 위한 물리 채널의 주파수 및 부호 정보와, 기지국에서 제공 가능한 방송 서비스들을 나타내는 BCS ID(Broadcast Service Identifier) 등의 방송 서비스 파라미터를 포함한다. 단말은 상기 방송

서비스 파라미터에 의해 논리적 방송 서비스 정보와 물리채널 사이의 매핑 여부를 확인하고, 해당 물리채널을 액세스한다.

<43> 단말은 BSPM에 포함된 n개의 방송 서비스들에 대한 BCS ID들, BCS1, BCS2, ... BCSn 중 원하는 방송 서비스의 BCS ID, 예를 들어 BCS2를 획득하고, 마찬가지로 상기 BSPM을 통해 알아낸 해당 서비스 주파수(f_{BCS2})로 전환한 후 상기 서비스 주파수에서 순방향 방송채널(Forward Broadcast Service Channel: F-BSCH)을 통해 방송 데이터를 수신한다. 단말 사용자가 방송 서비스를 종료하기를 원한다면 단말은 f_{BCS2}의 모니터링을 중지하고 원래의 주파수인 f_{HASH}로 되돌아간다. 음영으로 표시된 부분은 단말이 방송서비스를 받고 있는 시간구간을 나타낸다.

<44> 이동통신 시스템으로 제공되는 방송 데이터는 방송용 채널을 이용해 무선으로 방송된다. 이러한 방송 서비스에서 시스템 사용자 측면에서 중대하게 요구되는 특징은 인증되지 않은 단말 또는 불법적인 단말이 방송 데이터를 수신할 수 없도록 하는 것이다. 게다가 단말은 방송서비스 도중에도 음성 호 서비스를 위한 착신 요구, 즉 시스템에 의한 호출 신호를 받을 수 있어야 한다.

<45> 따라서 본 발명에 따른 방송서비스 시스템에서는 방송 데이터 트래픽을 소정 유효시간 동안 해당하는 암호화 키를 가지고 복호가 가능하도록 암호화하여 전송하고, 방송 서비스 도중 주기적 또는 비주기적으로 위치등록을 수행하는 이동 단말들에게 방송 데이터 트래픽의 복호를 위한 암호화 키를 제공한다. 이는 방송 서비스를 제공받는 이동 단말들에게 위치등록을 수행하도록 강제함으로써, 불법적인 사용을 방지하고 착신 요구를 정상적으로 수신할 수 있도록 하기 위함이다.

<46> 위치등록은 시스템과 단말 사이에 미리 약속된 등록 메시지를 기지국으로 전송함으로써 이루어진다. 도 4는 본 발명에 따른 위치등록 메시지의 포맷을 나타낸 것이다. 상기 도 4를 참

조하여 위치등록 메시지의 주요 필드들을 살펴보며, REG_TYPE 필드는 위치등록 이유를 나타내고, NUM_BCS_SESSION은 방송 서비스를 위해 연결된 세션 개수를 나타내고, 상기 세션 개수에 따라 방송 서비스를 위한 필드들이 이어진다. 방송 서비스를 위한 필드들로는 요구되는 방송 서비스의 내용을 나타내는 BCS_ID 필드와 방송 서비스의 종료 여부를 나타내는 DE_REG_IND가 있다.

<47> 단말의 위치등록은 시간제 등록(Time Based Registration), 시스템의 호출 메시지에 의한 지시된 등록(Ordered Registration) 또는 암호화 키의 유효시간 종료 등의 소정 위치등록 조건이 만족될 때에 이루어지며, 시스템은 위치등록 메시지의 REG_TYPE 필드로서 단말이 위치등록을 수행하는 이유를 구별한다. 상기 REG_TYPE 필드의 값들을 간단히 설명하면, '0000'은 이동 단말이 미리 정해지는 위치등록 주기에 도달하였을 때, '0001'은 전원이 켜졌을 때, '0010'은 새로운 위치등록 영역(Registration Zone)으로 진입할 때, '0011'은 전원이 꺼질 때, '0100'은 파라미터가 변경되었을 때, '0101'은 시스템으로부터 위치등록이 지시되었을 때, '0110'은 기지국으로부터의 거리가 소정 단위로 변화할 때, '0111'은 새로운 사용자 영역으로 진입하였을 때 위치등록을 수행함을 의미한다. 또한 '1000'은 방송서비스를 개시하거나 유지하기 위한 위치등록을 의미한다.

<48> 본 발명에 따르면 방송 서비스의 개시를 위한 위치등록에 응답하는 암호화는 기지국 또는 패킷 데이터 서비스 노드에서 이루어질 수 있으며, 이하 이를 두 가지의 실시예로 구분하여 설명하기로 한다.

<49> 도 5는 본 발명의 제1 실시예에 따라 기지국에 의해 단말의 등록을 수행하는 동작을 나타낸 메시지 흐름도이다. 여기에서 단말은 방송 서버로부터 방송 서버와 세션을 연결하기 위해 필요한 방송용 서비스 파라미터를 BSPM을 통해 이미 수신한 것으로 한다.

<50> 상기 도 5를 참조하면, 과정(a)에서 단말은 방송 서비스를 요구하기 위해 기지국으로 등록 메시지를 전송한다. 상기 등록 메시지의 포맷은 앞서 언급한 도 4에 나타낸 바와 같다. 상기 등록 메시지는 단말의 위치를 이동통신 시스템으로 등록함과 동시에 수신하고자 하는 방송 서비스의 종류를 기지국으로 전달하며, 또한 본 발명에 따라 방송 서비스를 위한 암호화 키를 요구하기 위한 것이다. 단말의 위치는 상기 등록 메시지를 수신하여 시스템으로 전달하는 기지국의 식별자에 의하여 알려지며, 단말이 수신하고자 하는 방송 서비스의 종류는 상기 등록 메시지에 포함되는 BCS_ID 필드에 의해 알려진다.

<51> 과정(b)에서 기지국은 단말로부터 BCS_ID를 포함하는 등록 메시지를 최초로 수신하면, 단말로부터 방송 서비스가 요구된 것으로 판단하고 상기 BCS_ID에 해당하는 방송 서비스를 위해 현재 시점에서 유효한 암호화 키를 생성하여 데이터 버스트 메시지(Data Burst Message: DBM)에 실어 단말로 전송한다. 기지국은 상기 단말의 위치 정보를 교환기(도시하지 않음) 또는 AAA 서버로 전달하여 등록한다.

<52> 상기 데이터 버스트 메시지는 CDMA(Code Division Multiple Access) 시스템에서 페이징 채널(Paging Channel)이나 순방향 공통 제어 채널(Forward Common Control Channel: F-CCCH)을 통해 단문 메시지 등을 전송하기 위하여 사용되는 것으로서, 여기에서는 상기 암호화 키 전체 또는 상기 암호화 키를 생성하는데 사용되는 생성정보, 즉 시드(seed)와, 선택적으로 상기 암호화 키의 유효시간을 운반한다. 다른 경우 상기 암호화 키는 기지국이 아닌 별도의 개체에 의해서 생성되어 기지국으로 제공될 수 있다. 도 5에서 암호화 키는 X로 표기되었으며 미리 정해지는 소정의 유효시간을 가진다.

<53> 도 6은 본 발명에 따라 암호화 키를 포함하는 데이터 버스트 메시지의 포맷을 나타낸 것이다. 상기 도 6을 참조하여 데이터 버스트 메시지의 주요 필드들을 살펴보면, BURST_TYPE 필

드는 포함되는 데이터의 종류를 나타내며, NUM_FIELDS 필드는 이어지는 CHARi 필드에 포함되는 필드들의 개수를 나타낸다. 상기 BURST_TYPE 필드가 암호화 키를 전송하는 DBM 유형을 나타내는 미리 정해진 값을 가지는 경우의 CHARi 필드의 데이터 구조(Data Structure)를 도 6의 하부에 나타내었다.

<54> 도시한 CHARi 필드에서, NUM_BCS_SESSION 필드는 방송 서비스를 위해 연결된 세션 개수를 나타내고, 상기 세션 개수에 따라 방송 서비스를 위한 필드들이 이어진다. 방송 서비스를 위한 필드들로는 요구되는 방송 서비스의 내용을 나타내는 BCS_ID 필드와 암호화 키 또는 암호화 키의 생성 정보를 나타내는 ENCRYPTION_KEY 필드와 상기 암호화 키의 유효시간을 나타내는 ENCRYPTION_KEY_LIFETIME 필드가 있다. 상기 ENCRYPTION_KEY_LIFETIME 필드는 시스템 설계자의 선택에 따라 포함되거나 포함되지 않을 수 있다.

<55> 다른 경우, 상기 BURST_TYPE 필드는 통상의 데이터 버스트 유형을 나타내는 값으로 설정되고 CHARi 필드는 패킷 데이터 서비스 노드로부터 단말로 전달되는 IP 패킷을 담을 수 있다. 이 경우 단말은 상기 IP 패킷의 내용을 분석하여 암호화 키를 추출한다.

<56> 과정(c)에서 단말은 상기 암호화 키를 성공적으로 수신하거나 또는 상기 시드를 수신하여 상기 암호화 키를 성공적으로 생성하면 기지국으로 긍정응답(Acknowledge: Ack) 메시지를 전송한다. 과정(d)에서 기지국은 단말로부터 Ack 메시지를 수신하면 상기 암호화 키가 성공적으로 수신된 것으로 판단하여, 현재의 시간으로 설정된 단말의 시간 스탬프(time stamp) 정보와 상기 BCS_ID를 IOS(Inter Operability Specification) 메시지에 실어 패킷 데이터 서비스 노드로 전송한다. 만일 단말로부터 암호화 키를 포함하는 데이터 버스트 메시지에 대한 응답이 수신되지 않으면 기지국은 단말로부터 응답이 수신될 때까지 미리 지정된 회수만큼 상기 암호화 키를 포함하는 데이터 버스트 메시지를 재전송한다.

<57> 과정 (e)에서 패킷 데이터 서비스 노드는 상기 IOS 메시지에 응답하여 단말기 별로 방송 서비스 접속 시간에 대한 정보, 즉 과금 정보를 과금 요구(Accounting Request) 메시지에 실어 AAA 서버로 전송한다. 그러면 과정(f)에서 AAA 서버는 상기 과금 정보를 저장하고 응답(Accounting Reply) 메시지를 패킷 데이터 서비스 노드로 전송하며, 과정(g)에서 패킷 데이터 서비스 노드는 Ack 메시지를 기지국으로 전송하여 과금 처리가 수행되었음을 알린다.

<58> 과정(h)에서 기지국은 패킷 데이터 서비스 노드를 통해 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 방송 서비스 채널을 통해 단말로 전송한다. 그러면 단말은 상기 수신한 암호화 키를 가지고 상기 방송 데이터를 복호한다. 하기에 간략화된 방송 데이터의 암호화 수식을 나타내었다.

<59> 암호화된 방송 데이터 = DES(X key, 방송 데이터)

<60> 보다 구체적으로 설명하면, 기지국 제어기(BSC)는 단말의 등록 메시지에 응답하여 암호화 키를 생성하고 상기 생성된 암호화 키의 정보를 단말로 전송하며, 방송 서버로부터 패킷 데이터 서비스 노드를 통해 제공되는 방송 데이터는 기지국의 제2 계층에 해당하는 기지국 송수신기(BTS)에서 암호화된 후 단말로 전송된다.

<61> 상기 암호화 키는 해당 유효시간이 종료되면 사용할 수 없다. 매 유효시간이 종료될 때마다 기지국 제어기(BSC)는 새로운 암호화 키를 생성하며, 기지국 송수신기는 상기 새로운 암호화 키에 의해 암호화된 방송 데이터를 전송한다. 따라서 단말은 암호화 키의 유효시간이 종료되면 등록 메시지를 전송하여 새로운 암호화 키를 수신한다. 상기 암호화 키의 유효시간은 해당 암호화 키와 함께 데이터 버스트 메시지를 통해 수신한다.

<62> 이상에서 설명한 바와 같이 단말은 방송 서비스를 진행하는 동안 소정의 위치등록 조건이 만족될 때마다 반복적으로 등록 메시지를 전송하고 그에 대한 응답으로 암호화 키를 수신하며, 기지국은 암호화 키의 전송에 성공할 때마다 패킷 데이터 서비스 노드를 통해 AAA 서버로 과금 정보를 전송한다. 그러면 결국 적어도 암호화 키의 유효시간 마다 과금 정보가 발생되며 이러한 빈번한 발생은 시스템의 부하를 가중시키는 원인이 된다. 따라서 본 발명의 변형된 실시예에 따른 기지국 또는 패킷 데이터 서비스 노드는 소정 개수의 과금 정보를 수집하여 한꺼번에 AAA 서버로 제공하거나, 또는 단말이 방송 서비스를 종료하였을 때까지 과금 정보를 한꺼번에 AAA 서버로 제공한다. 이때 기지국은 암호화 키의 유효시간이 종료된 후 소정 시간이 경과될 때까지 단말로부터 등록 메시지가 수신되지 않으면 단말이 방송 서비스를 종료한 것으로 판단할 수 있다.

<63> 도 7은 본 발명의 제2 실시예에 따라 패킷 데이터 서비스 노드(PDSN)에 의해 단말의 등록을 수행하는 동작을 나타낸 메시지 흐름도이다. 여기에서 단말은 방송 서버로부터 방송 서버와 세션을 연결하기 위해 필요한 방송용 서비스 파라미터를 BSPM을 통해 이미 수신한 것으로 한다.

<64> 상기 도 7을 참조하면, 과정(a)에서 단말은 방송 서비스를 요구하기 위해 기지국으로 등록 메시지를 전송한다. 상기 등록 메시지의 포맷은 앞서 언급한 도 4에 나타낸 바와 같다. 상기 등록 메시지는 단말의 위치를 이동통신 시스템으로 등록함과 동시에 수신하고자 하는 방송 서비스의 종류를 기지국으로 전달하며, 또한 본 발명에 따라 방송 서비스를 위한 암호화 키를 요구하기 위한 것이다. 단말의 위치는 상기 등록 메시지를 수신하여 시스템으로 전달하는 기지

국의 식별자에 의하여 알려지며, 단말이 수신하고자 하는 방송 서비스의 종류는 상기 등록 메시지에 포함되는 BCS_ID 필드에 의해 알려진다.

<65> 과정(b)에서 기지국은 단말로부터 BCS_ID를 포함하는 등록 메시지를 최초로 수신하면 단말로부터 방송 서비스가 요구된 것으로 판단하고 자동적으로 L2 Ack 메시지로 응답하는 동시에 상기 단말의 위치 정보를 교환기(도시하지 않음) 또는 AAA 서버로 전달하여 등록한다. 그리고 과정(c)에서 기지국은 현재의 시간으로 설정된 단말의 시간 스탬프(time stamp) 정보와 상기 BCS_ID를 IOS 메시지에 실어 패킷 데이터 서비스 노드로 전송한다.

<66> 과정 (d)에서 패킷 데이터 서비스 노드는 상기 IOS 메시지에 응답하여 단말기 별로 방송 서비스 접속 시간에 대한 정보, 즉 과금 정보를 과금 요구(Accounting Request) 메시지에 실어 AAA 서버로 전송한다. 그러면 과정(e)에서 AAA 서버는 상기 과금 정보를 저장하고 응답(Accounting Reply) 메시지를 패킷 데이터 서비스 노드로 전송한다. 제1 실시예에서와 마찬가지로 패킷 데이터 서비스 노드는 소정 개수의 과금 정보를 수집하여 한꺼번에 AAA 서버로 제공하거나, 또는 단말이 방송 서비스를 종료하였을 때까지 수집된 과금 정보를 한꺼번에 AAA 서버로 제공한다.

<67> 상기한 과금 처리가 완료된 후, 과정(f)에서 패킷 데이터 서비스 노드는 상기 BCS_ID에 해당하는 방송 서비스를 위해 현재 시점에서 유효한 암호화 키를 생성하고 상기 과금 처리가 성공적으로 수행되었음을 알리는 Ack 메시지에 상기 암호화 키의 정보를 실어 기지국으로 전송한다. 상기 패킷 데이터 서비스 노드는 상기 암호화 키 전체를 전송하거나 또는 상기 암호화 키를 생성하는데 사용되는 생성 정보, 즉 시드를 전송할 수 있다.

<68> 과정(g)에서 기지국은 상기 패킷 데이터 서비스 노드로부터 수신한 상기 암

호화 키 또는 상기 생성 정보를 데이터 버스트 메시지(DBM)에 실어 단말로 전송한다. 도 7에서 암호화 키는 X로 표기되었으며 미리 정해지는 소정의 유효시간을 가진다. 본 발명에 따라 암호화 키를 포함하는 상기 데이터 버스트 메시지의 포맷은 앞서 언급한 도 6에 나타낸 바와 같다. 또한 마찬가지로 상기 데이터 버스트 메시지는 상기 암호화 키 또는 상기 시드를 적어도 포함하며, 선택적으로 상기 암호화 키의 유효시간을 포함한다.

<69> 과정(h)에서 단말은 상기 암호화 키를 성공적으로 수신하거나 또는 상기 시드를 수신하여 상기 암호화 키를 성공적으로 생성하면 기지국으로 Ack 메시지를 전송하여 상기 암호화 키가 성공적으로 수신되었음을 알린다. 과정(i)에서 패킷 데이터 서비스 노드는 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 기지국을 통해 단말로 전송한다. 그러면 단말은 상기 수신한 암호화 키를 가지고 상기 방송 데이터를 복호한다.

<70> 즉, 기지국은 단말의 등록 메시지에 응답하여 패킷 데이터 서비스 노드로부터 제공받은 암호화 키를 단말로 전송하며, 방송 서버로부터 제공되는 방송 데이터는 패킷 데이터 서비스 노드에서 암호화된 후 기지국을 통해 단말로 전송된다.

<71> 제1 실시예에서와 마찬가지로 상기 암호화 키는 해당 유효시간이 종료되면 사용할 수 없다. 매 유효시간이 종료될 때마다 패킷 데이터 서비스 노드는 새로운 암호화 키를 생성하고, 상기 새로운 암호화 키에 의해 암호화된 방송 데이터를 전송한다. 따라서 단말은 암호화 키의 유효시간이 종료되면 등록 메시지를 전송하여 새로운 암호화 키를 수신한다. 상기 암호화 키의 유효시간은 해당 암호화 키와 함께 데이터 버스트 메시지를 통해 수신한다.

<72> 한편, 이상에서는 단말의 등록 메시지를 수신한 기지국이 암호화 키에 관련된 정보를 단문 메시지의 전송에 이용되는 데이터 버스트 메시지(DBM)에 실어 전송하는 것으로 설명하였으나, 다른 경우 암호화 정보는 도 8에 나타낸 바와 같은 전용의 암호화 정보 메시지(Encryption Information Message: EIM)에 실려 전송될 수 있다.

<73> 상기 도 8을 참조하여 암호화 정보 메시지의 주요 필드들을 살펴보면, NUM_BCS_SESSION 필드는 방송 서비스를 위해 연결된 세션 개수를 나타내고, 상기 세션 개수에 따라 방송 서비스를 위한 필드들이 이어진다. 방송 서비스를 위한 필드들로는 요구되는 방송 서비스의 내용을 나타내는 BCS_ID 필드와 암호화 키 또는 암호화 키의 생성 정보를 나타내는 ENCRYPTION_KEY 필드와 상기 암호화 키의 유효시간을 나타내는 ENCRYPTION_KEY_LIFETIME 필드가 있다. 상기 ENCRYPTION_KEY_LIFETIME 필드는 시스템 설계자의 선택에 따라 포함되거나 포함되지 않을 수 있다.

<74> 한편 본 발명의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시예에 국한되지 않으며, 후술되는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

【발명의 효과】

<75> 이상에서 상세히 설명한 바와 같이 동작하는 본 발명에 있어서, 개시되는 발명중 대표적인 것에 의하여 얻어지는 효과를 간단히 설명하면 다음과 같다.

<76> 본 발명은, 방송 서비스 시 단말의 등록(Registration)을 의무화시킴으로써 규칙적인 방송 서비스 등록을 통한 단말의 방송 서비스의 수신 시간을 과금에 활용할 수 있다. 또한 무선 구간을 통해 방송 서비스를 제공하는 시스템에서 불법적인 사용자에 의한 방송 서비스의 사용을 방지하고 정확한 과금 정보를 수집할 수 있다.

【특허청구범위】

【청구항 1】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 단말에서 방송 서비스를 제공받는 방법에 있어서,

상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 생성하여 상기 기지국으로 전송하는 과정과,

상기 등록 메시지에 응답하여 방송 서비스를 위해 소정 유효시간을 가지는 암호화 키를 포함하는 암호화 정보 메시지를 수신하는 과정과,

방송 서비스 채널을 통해 상기 기지국으로부터 수신한 방송 데이터를 상기 암호화 정보 메시지에 포함된 암호화 키를 가지고 복호화하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 2】

제 1 항에 있어서, 상기 유효시간이 종료되면 새로운 암호화 키를 수신하기 위한 등록 메시지를 생성하여 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 3】

제 1 항에 있어서, 상기 암호화 정보 메시지는, 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자와, 상기 암호화 키와, 상기 암호화 키의 유효시간을 나타내는 정

보를 포함하는 것을 특징으로 하는 상기 방법.

【청구항 4】

제 1 항에 있어서, 상기 등록 메시지는, 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자와, 상기 위치 등록을 수행하는 이유를 포함하는 것을 특징으로 하는 상기 방법.

【청구항 5】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 수신하는 과정과,

상기 등록 메시지에 응답하여 방송 서비스를 위해 소정 유효시간을 가지는 암호화 키를 생성하고 상기 생성된 암호화 키를 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정과,

상기 패킷 데이터 서비스 노드를 통해 상기 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 6】

제 5 항에 있어서, 상기 암호화 정보 메시지는, 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자와, 상기 암호화 키와, 상기 암호화 키의 유효시간을 나타내는 정보를 포함하는 것을 특징으로 하는 상기 방법.

【청구항 7】

제 5 항에 있어서, 상기 등록 메시지는, 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자와, 상기 위치 등록을 수행하는 이유를 포함하는 것을 특징으로 하는 상기 방법.

【청구항 8】

제 5 항에 있어서, 상기 암호화 정보 메시지를 전송한 후 상기 단말로부터 상기 암호화 정보 메시지가 성공적으로 수신되었음을 알리는 응답 메시지가 수신되면, 현재 시간으로 설정된 단말의 시간 스탬프 정보와 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자를 포함하는 과금 정보를 생성하여, 상기 패킷 데이터 네트워크에 연결되어 상기 단말의 과금을 처리하는 인증 및 과금 서버에게 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 9】

제 5 항에 있어서, 상기 암호화 정보 메시지를 전송한 후 상기 단말로부터 상기 암호화 정보 메시지가 성공적으로 수신되었음을 알리는 응답 메시지가 수신되면, 현재 시간으로 설정

된 단말의 시간 스탬프 정보와 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자를 포함하는 과금 정보를 생성하는 과정과,

미리 정해지는 주기마다 상기 과금 정보를 수집하여, 상기 패킷 데이터 네트워크에 연결되어 상기 단말의 과금을 처리하는 인증 및 과금 서버에게 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 10】

제 5 항에 있어서, 상기 암호화 정보 메시지를 전송한 후 상기 단말로부터 상기 암호화 정보 메시지가 성공적으로 수신되었음을 알리는 응답 메시지가 수신되면, 현재 시간으로 설정된 단말의 시간 스탬프 정보와 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자를 포함하는 과금 정보를 생성하는 과정과,

상기 단말에서 방송 서비스의 수신을 종료하면, 상기 방송 서비스 동안의 과금 정보를 수집하여, 상기 패킷 데이터 네트워크에 연결되어 상기 단말의 과금을 처리하는 인증 및 과금 서버에게 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 11】

제 10 항에 있어서, 상기 단말로부터 주기적인 등록 메시지가 수신되지 않으면 상기 단말에서 방송 서비스의 수신을 종료한 것으로 판단하는 것을 특징으로 하는 상기 방법.

【청구항 12】

무선 채널을 통해 단말에게 방송 서비스를 제공하는 기지국과 상기 기지국을 패킷 데이터 네트워크를 통해 방송 서버로 연결하는 패킷 데이터 서비스 노드를 포함하는 이동통신 시스템에서 상기 기지국과 상기 패킷 데이터 서비스 노드에 의해 상기 단말에게 방송 서비스를 제공하는 방법에 있어서,

상기 기지국에서 상기 단말로부터 상기 이동통신 시스템에 방송 서비스의 제공을 요청하기 위한 등록 메시지를 수신하고, 현재 시간으로 설정된 단말의 시간 스탬프 정보와 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자를 포함하는 과금 정보를 생성하여 상기 패킷 데이터 서비스 노드로 전송하는 과정과,

상기 패킷 데이터 서비스 노드에서 상기 기지국으로부터 상기 과금 정보를 수신하여, 방송 서비스를 위해 소정 유효시간을 가지는 암호화 키를 생성하고 상기 생성된 암호화 키를 상기 기지국으로 제공하는 과정과,

상기 기지국에서 상기 패킷 데이터 서비스 노드로부터 상기 암호화 키를 수신하여, 상기 암호화 키를 포함하는 암호화 정보 메시지를 상기 단말로 전송하는 과정과,

상기 패킷 데이터 서비스 노드에서 상기 방송 서버로부터 수신한 방송 데이터를 상기 암호화 키를 가지고 암호화하여 상기 기지국을 통해 상기 단말로 전송하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

【청구항 13】

제 12 항에 있어서, 상기 암호화 정보 메시지는, 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자와, 상기 암호화 키와, 상기 암호화 키의 유효시간을 나타내는 정보를 포함하는 것을 특징으로 하는 상기 방법.

【청구항 14】

제 12 항에 있어서, 상기 등록 메시지는, 상기 단말에서 수신하는 방송 서비스를 나타내는 방송 서비스 식별자와, 상기 위치 등록을 수행하는 이유를 포함하는 것을 특징으로 하는 상기 방법.

【청구항 15】

제 12 항에 있어서, 상기 패킷 데이터 서비스 노드에서 상기 기지국으로부터 수신한 상기 과금 정보를, 상기 패킷 데이터 네트워크에 연결되어 상기 단말의 과금을 처리하는 인증 및 과금 서버에게 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 16】

제 12 항에 있어서, 상기 패킷 데이터 서비스 노드에서 미리 정해지는 주기동안의 과금 정보를 상기 기지국으로부터 수집하여, 상기 패킷 데이터 네트워크에 연결되어 상기 단말의 과금을 처리하는 인증 및 과금 서버에게 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 17】

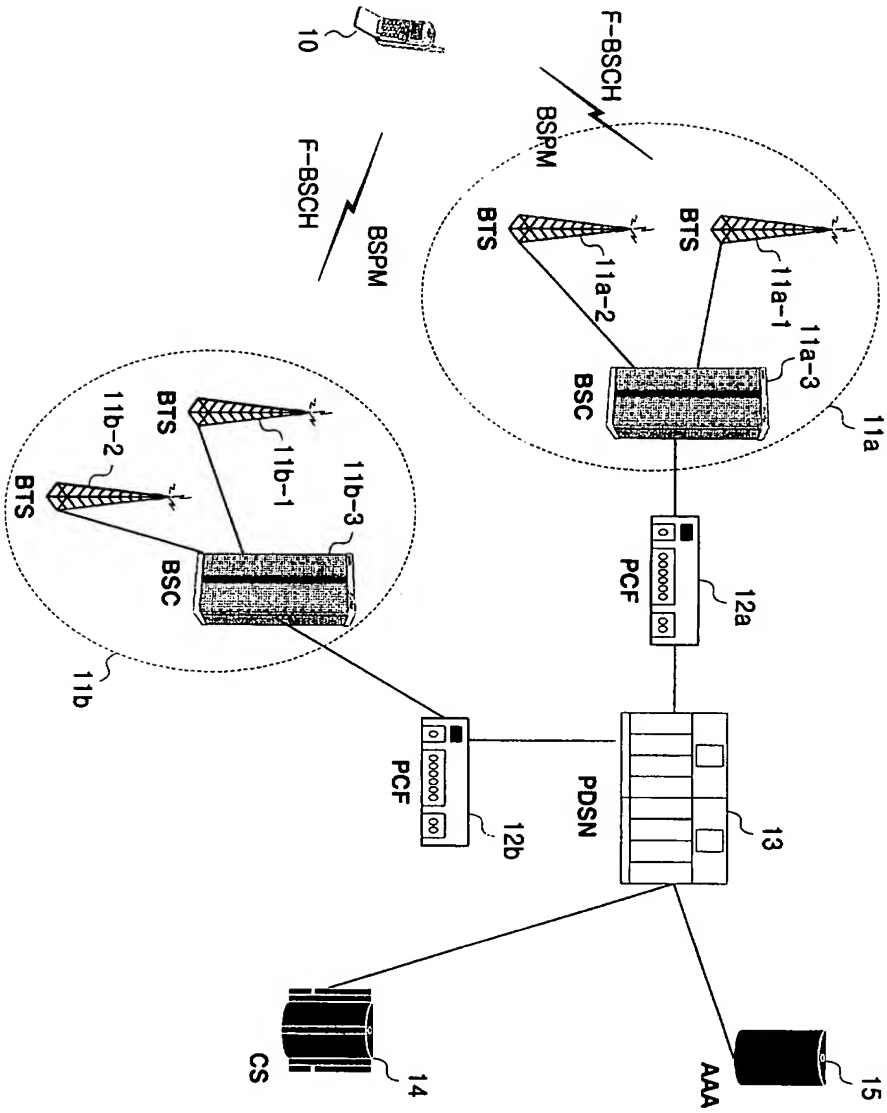
제 12 항에 있어서, 상기 단말에서 방송 서비스의 수신을 종료하면, 상기 패킷 데이터 서비스 노드에서 상기 방송 서비스 동안의 과금 정보를 상기 기지국으로부터 수집하여, 상기 패킷 데이터 네트워크에 연결되어 상기 단말의 과금을 처리하는 인증 및 과금 서버에게 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

【청구항 18】

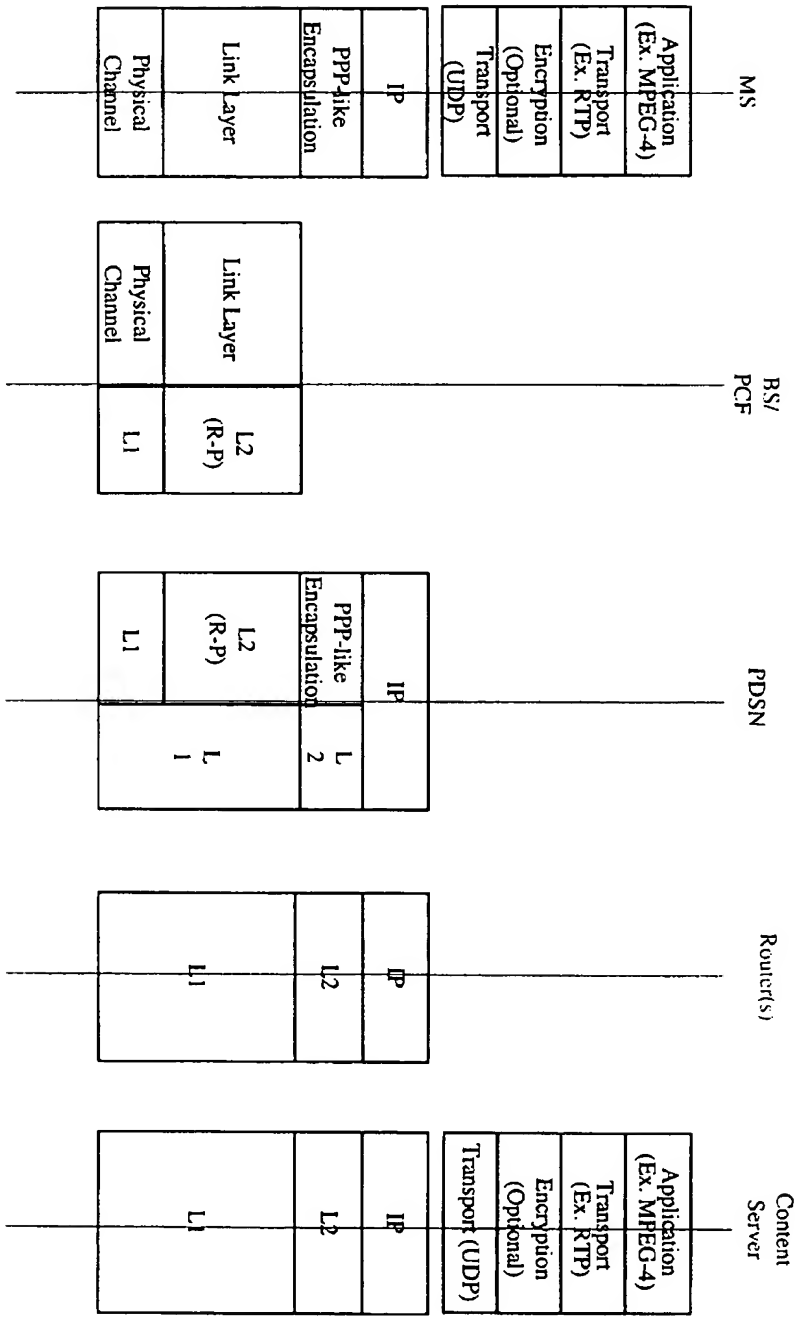
제 17 항에 있어서, 상기 단말로부터 상기 기지국으로 주기적인 등록 메시지가 수신되지 않으면 상기 단말에서 방송 서비스의 수신을 종료한 것으로 판단하는 것을 특징으로 하는 상기 방법.

【도면】

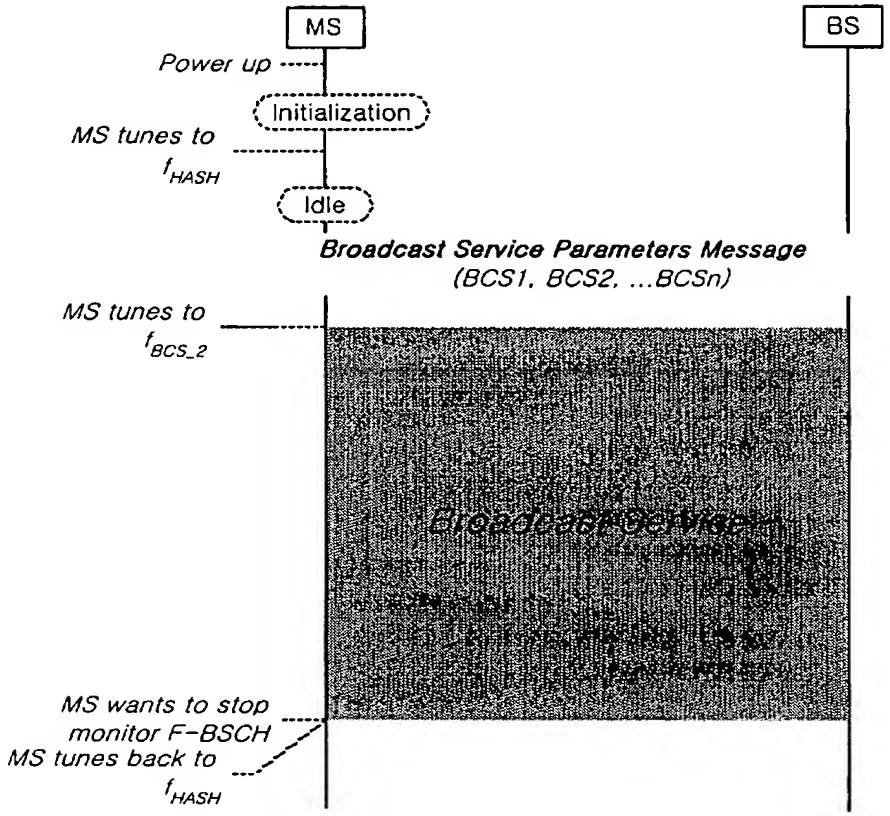
【도 1】


10
F-BSCH
BSPM
F-BSCH
BSPM
BTS
BTS
11a-2
11a-1
11a-3
BSC
11a
BTS
BTS
11b-2
11b-1
11b-3
BSC
11b
PCF
12a
PCF
12b
PDSN
13
CS
14
AAA
15

【도 2】


MS
Application (Ex. MPEG-4)
Transport (Ex. RTP)
Encryption (Optional)
Transport (UDP)
IP
PPP-like Encapsulation
Link Layer
Physical Channel
BS/ PCF
Link Layer
L2 (R-P)
Physical Channel
L1
PDSN
IP
PPP-like Encapsulation
L2 (R-P)
L1
L2
L1
Router(s)
IP
L2
L1
Content Server
Application (Ex. MPEG-4)
Transport (Ex. RTP)
Encryption (Optional)
Transport (UDP)
IP
L2
L1

【도 3】


MS
BS
Power up
Initialization
MS tunes to
f_{HASH}
Idle
Broadcast Service Parameters Message
(BCS1, BCS2, ...BCSn)
MS tunes to
f_{BCS_2}
MS wants to stop
monitor F-BSCH
MS tunes back to
f_{HASH}

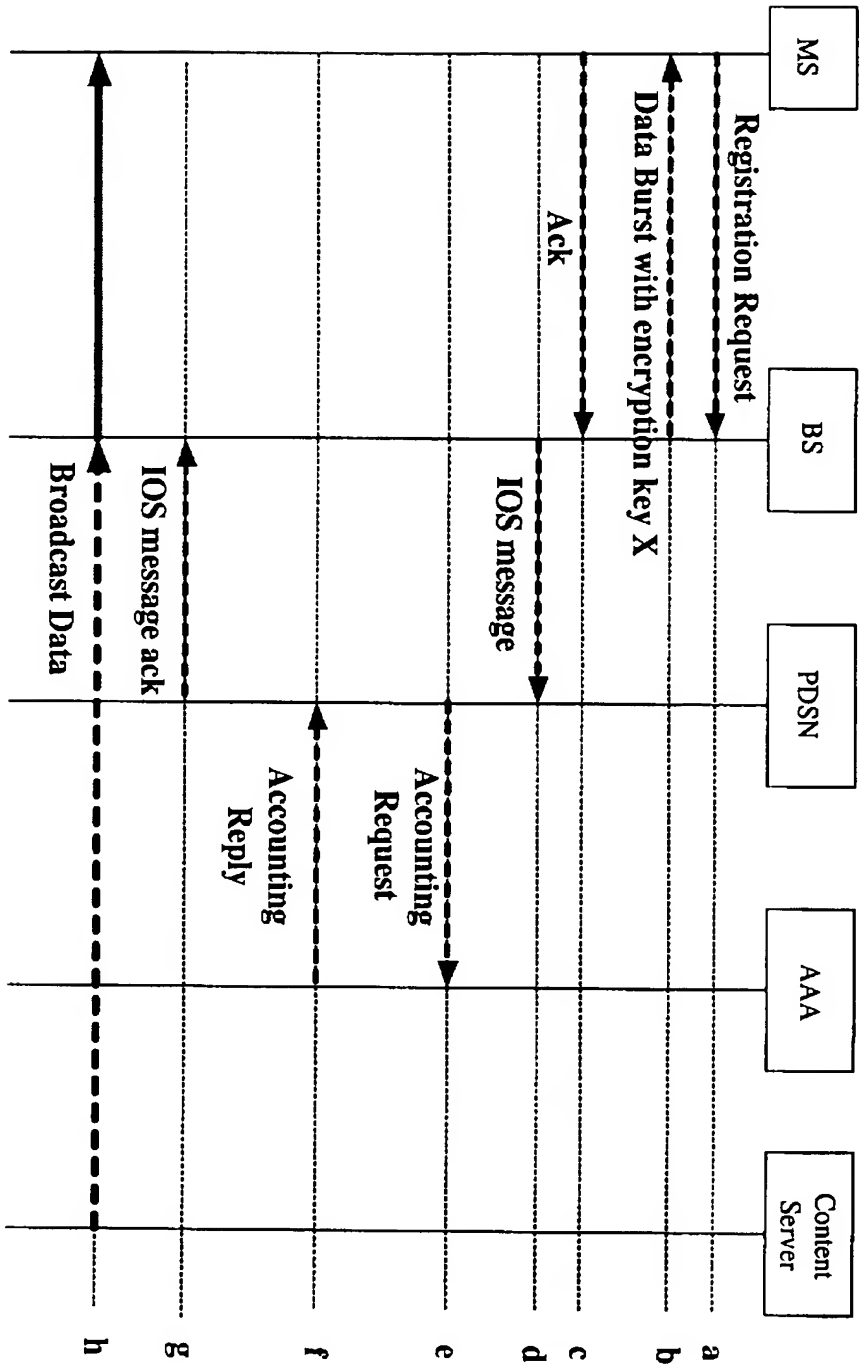
【도 4】

REGISTRATION MESSAGE

FIELD	**LENGTH (bits)**
REG_TYPE	4
...	
NUM_BCS_SESSION	0 or 6
NUM_BCS_SESSION occurrences of the following field	
BCS_ID	32
DE_REG_IND	1

REG_TYPE(binary)	Type of Registration
0000	Timer based
0001	Power up
0010	Zone based
0011	Power down
0100	Parameter change
0101	Ordered
0110	Distance based
0111	User Zone based
1000	BCS Session
...	reversed

【도 5】


MS
BS
PDSN
AAA
Content Server
Registration Request
Data Burst with encryption key X
Ack
IOS message
Accounting Request
Accounting Reply
IOS message ack
Broadcast Data
a
b
c
d
e
f
g
h

【도 6】

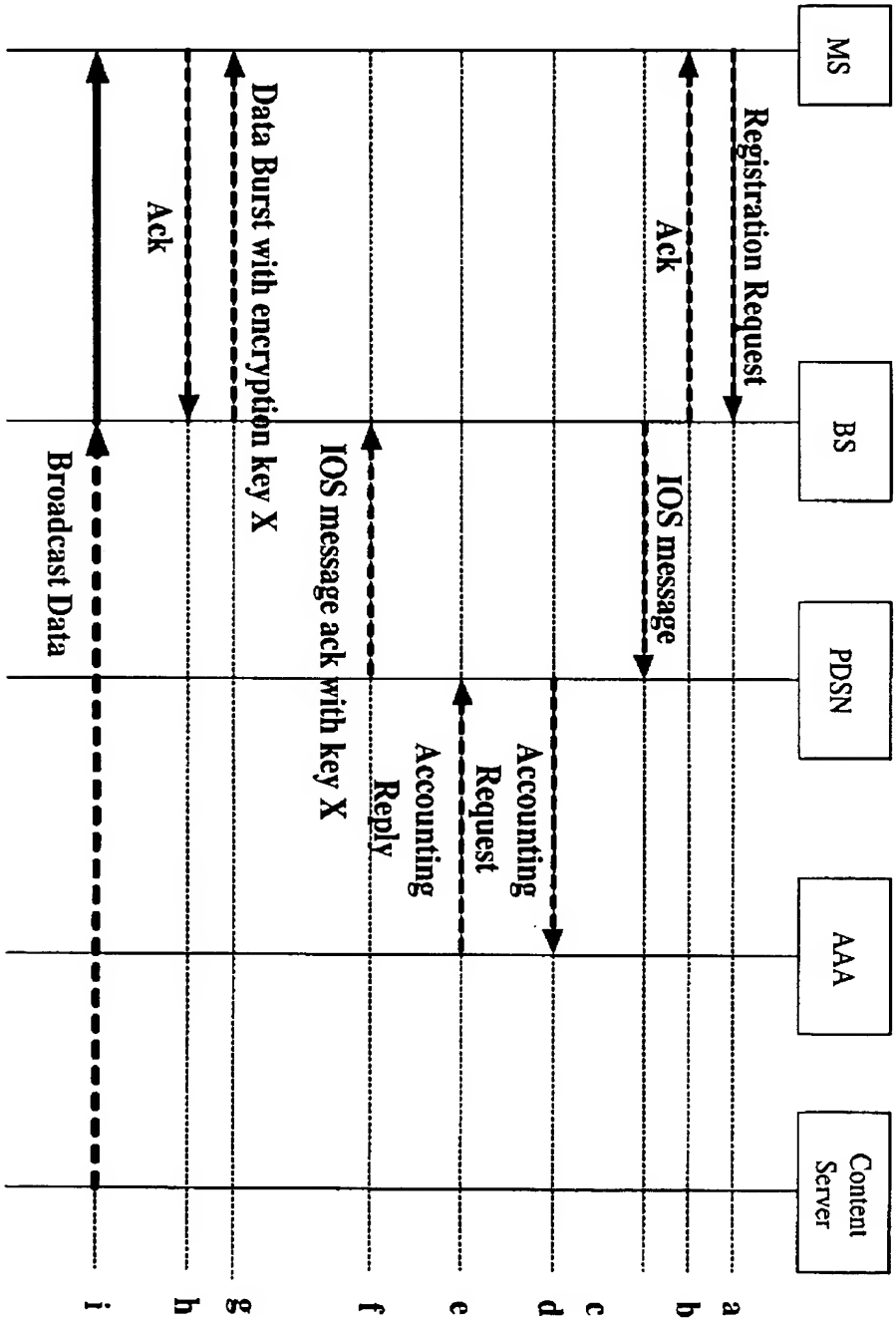
DATA BURST MESSAGE (DBM)

FIELD	**LENGTH (bits)**
MSG_NUMBER	8
BURST_TYPE	6
NUM_MSGS	8
NUM_FIELDS	8
NUM_FIELDS occurrences of the following field	
CHARi	8

CHARi FIELD

NUM_BCS_SESSION	6
NUM_BCS_SESSION occurrences of the following fields:	
BCS_ID	32
ENCRYPTION_KEY	8
ENCRYPTION_KEY_LIFETIME	12

【도 7】


MS
BS
PDSN
AAA
Content Server
Registration Request
Ack
IOS message
Accounting Request
Accounting Reply
IOS message ack with key X
Data Burst with encryption key X
Ack
Broadcast Data
a
b
c
d
e
f
g
h
i

【도 8】

ENCRYPTION INFORMATION MESSAGE (EIM)

FIELD	**LENGTH (bits)**
NUM_BCS_SESSION	6
NUM_BCS_SESSION occurrences of the following fields:	
BCS_ID	32
ENCRYPTION_KEY	8
ENCRYPTION_KEY_LIFETIME	12